ABSTRACT

The invention combines cryptographic key management technology with various authentication options and the use of a companion PKI system in a web-centric cryptographic key management security method and apparatus called *PXa³™ (Precise eXtensible Authentication, Authorization and Administration).* The *PXa³* model uses a security profile unique to a network user and the member domain(s) he/she belongs to. A PXa³ server holds all private keys and certificates, the user's security profile, including credentials and the optional authentication enrollment data. The server maintains a security profile for each user, and administrators simply transmitted credential updates and other periodic maintenance updates to users via their PXa³ server-based member accounts. Domain and workgroup administrators also perform administrative chores via a connection to the *PXa³* web site, rather than on a local workstation. A member's security profile, containing algorithm access permissions, credentials, domain and maintenance values, a file header encrypting key, optional biometric templates, and domain-specific policies is contained in one of two places: either on a removable cryptographic token (*e.g.*, a smart card), or on a central server-based profile maintained for each member and available as a downloadable "soft token" over any Internet connection.